# Audit Report

**OIG-05-041**

**INFORMATION TECHNOLOGY: FMS's Computer Security Incident Response Capability Needs Improvement**

**July 13, 2005**

Office of
Inspector General

Department of the Treasury

# Contents



## Abbreviations

| | |
|---|---|
| CIO | Chief Information Officer |
| CSIRC | Computer Security Incident Response Capability |
| FISMA | Federal Information Security Management Act |
| FMS | Financial Management Service |
| FY | Fiscal Year |
| GISRA | Government Information Security Reform Act |
| IDS | Intrusion Detection System |
| IR | Information Resources |
| IT | Information Technology |
| MAD | Mission Assurance Directorate |
| NIST | National Institute of Standards and Technology |
| OIG | Office of Inspector General |
| OMB | Office of Management and Budget |
| PCB | Patch Control Board |
| TCSIRC | Treasury's Computer Security Incident Response Center |
| TD P | Treasury Directive Publication |
| Treasury | Department of the Treasury |

Richard L. Gregg
Commissioner
Financial Management Service

The Office of Inspector General's (OIG) Annual Plan for Fiscal Year (FY) 2004 included the audit project, *Independent Evaluation of Treasury's Information Security Program and Practices Pursuant to the Federal Information Security Management Act (FISMA)*. As part of this review, the OIG was required to evaluate aspects of the Department of the Treasury's (Treasury) computer security incident response capability (CSIRC). During our FY 2003 FISMA independent evaluation, we noted that the number of computer security incidents reported by Treasury bureaus varied significantly. The Office of Management and Budget (OMB) reported similar divergence in incidents reported across Federal agencies in its FY 2003 FISMA report to Congress in March 2004.

This audit was structured based on current, as well as prior, OMB FISMA reporting requirements. The OIG also plans to incorporate the results of this audit into its FY 2005 FISMA evaluation. This audit is also consistent with Treasury Directive Publication (TD P) 85-01, *Treasury Information Technology Security Program*[1], which requires that Treasury bureaus establish and maintain an incident response capability.

Our overall objective for this audit was to determine if the Financial Management Service (FMS) established an adequate CSIRC process. To accomplish this objective, we: (1) interviewed FMS information technology (IT) personnel; (2) reviewed relevant IT policy and procedure documents; and (3) observed the actual IT reporting processes that produce CSIRC and software patch management data. A more detailed description of our objective, scope, and methodology is provided in Appendix 1.

[1] *Treasury IT Security Program* (TD P 85-01) was updated as of August 15, 2003

## Results In Brief

Overall, we found that although FMS did establish a CSIRC and a software patch management function, its computer security incident reporting process can be improved. For instance, we identified that: (1) current CSIRC policy and procedures were not complete; (2) Help Desk computer security incident reporting was not complete; (3) a monthly virus scan was not performed for April 2004; (4) potential incident investigations were not always completed; and (5) software patch management procedures were not complete.

Our report includes several recommendations that, in our opinion, will assist FMS in strengthening its CSIRC function. Specifically, we are recommending that the FMS's Chief Information Officer (CIO) ensure that:

1. Current FMS CSIRC policy and procedures are revised to incorporate bureau head responsibilities; and subsequent incidents are reported to the Treasury's Computer Security Incident Response Center (TCSIRC).
2. All significant incidents identified by the Help Desk are reported to TCSIRC.
3. Help Desk tickets contain complete information; and follow-up tickets are generated for potential significant incidents identified by the Help Desk.
4. Virus scans are performed on a monthly basis.
5. All investigations of potential incidents identified by intrusion detection system (IDS) and firewall logs are completed.
6. Software patch management procedures are revised to include the requirements regarding current server software related patches; approved software for accessing the Internet; and repairing and mitigating vulnerabilities discovered during penetration testing.

## Background

According to the National Institute of Standards and Technology (NIST), computer security incident response has become an

important component of IT programs.[2] Security-related threats have become not only more numerous and diverse, but also more damaging and disruptive. New types of security-related incidents emerge frequently. Preventative activities based on the results of risk assessments can lower the number of incidents, but not all incidents can be prevented. An incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services.

NIST guidance also states that since performing incident response effectively is a complex undertaking, establishing a successful incident response capability requires substantial planning and resources.[3] Continually monitoring threats through an IDS is essential. Establishing clear procedures for assessing the current and potential business impact of incidents is critical, as is implementing effective methods of collecting, analyzing, and reporting data. Building relationships and establishing suitable means of communication with other internal groups (e.g., human resources, legal) and with external groups (e.g., other incident response teams, law enforcement) are also vital.

TCSIRC provides a means for: (1) receiving and/or disseminating computer security incident information to Treasury bureaus; and (2) a consistent capability to respond to, and report on, computer security incidents. See Appendix 2 for an overview of the TCSIRC structure and functionality.

As part of our fieldwork, we also performed a multi-year analysis of total number of computer security incidents reported to OMB as a result of the Government Information Security Reform Act (GISRA) and FISMA reporting. For its FY 2002 GISRA reporting, FMS reported one incident. For its FY 2003 FISMA reporting, FMS reported 1,669,663. The dramatic increase in the number of reported incidents was due to the IDS that FMS installed to monitor its network in the time between the FY 2002 GISRA and FY 2003 FISMA report.

[2] NIST Special Publication 800-61, "*Computer Security Incident Handling Guide*", dated January 2004.
[3] NIST Special Publication 800-61, "*Computer Security Incident Handling Guide",* dated January 2004.

## Finding and Recommendations

Although we identified areas where FMS can improve its current CSIRC process, we also identified areas where FMS was taking appropriate steps in establishing an adequate CSIRC and software patch management function. For example:

- FMS has established a full-time CSIRC program operated by the Security Operations Directorate and the Mission Assurance Directorate (MAD).
- The FMS CSIRC correctly distinguishes between computer security "events"[4] and computer security "incidents."[5] The FMS's CSIRC process also correctly classifies computer security incidents according to the requirements of TD P 85-01, and files monthly reports on a timely basis.
- FMS established a full-time software patch management function to address computer security vulnerabilities. The software patch management function is comprised of two components that address operating system security patches, and virus protection. The software patch management function is operated by the Information Resources (IR) Division, and is assisted by its Patch Control Board (PCB).
- The software patch management function subscribes to relevant vulnerability alert services.
- The Platform Engineering Division maintains a dedicated testing lab for testing patches prior to implementation.
- FMS developed an end-user, IT security awareness training program. This annual training is mandatory for all FMS computer users, including contractors.

[4] Per TD P 85-01, an "event" is a notable occurrence, not yet assessed, in a computing or telecommunications system or network that may affect that system or network.

[5] Per TD P 85-01, an "incident" is a violation of an explicit or implied security policy in a computing or telecommunications system or network.

## Finding 1 FMS's Computer Security Incident Response Capability Can Be Improved

Although FMS established a CSIRC and software patch management function, we identified areas where its computer security incident reporting process can be improved. More specifically, (1) current CSIRC policy and procedures were not complete; (2) Help Desk computer security incident reporting was not complete; (3) a monthly virus scan was not performed for FY 2004; (4) potential incident investigations were not always completed; and (5) software patch management procedures were not complete.

### FMS's CSIRC Policy and Procedures Were Not Complete

We found that FMS established policy and procedures for its CSIRC function. However, we identified areas in FMS's policy and procedures that did not include certain requirements identified in TD P 85-01. For instance, TD P 85-01 specifies that it is the responsibility of the bureau heads to: (1) establish a bureau CSIRC to serve as the first tier of incident response and the investigative and reporting body; (2) develop and maintain the bureau CSIRC policy and procedures; and (3) enforce the processes and procedures developed by the TCSIRC. These bureau head responsibilities were not defined in FMS's policy and procedures. In addition, TD P 85-01 requires that bureaus forward to TCSIRC, any relevant information that becomes available after an incident is closed. FMS's CSIRC policy and procedures do not specifically cite this responsibility.

### Help Desk Computer Security Incident Reporting Was Not Complete

FMS uses a tracking system to record its Help Desk tickets. For the month of April 2004, we selected and reviewed a sample of Help Desk tickets from the tracking system. During our review, we found a ticket addressing a significant incident, as well as another ticket citing a potentially significant incident. However, for the month of April 2004, FMS reported no significant incidents to TCSIRC. In addition, we found that follow-up tickets were not always created for the potentially significant incidents that we

reviewed. Also, for the sample of Help Desk tickets we reviewed, we found that some tickets did not contain complete information. For example, we identified tickets that were not completely filled out, particularly in the description section where nature of the event was not identified.

Virus Scan Was Not Performed For April 2004

We reviewed FMS's anti-virus logs and found that the weekly virus scans were not performed during the entire month of April 2004. FMS uses a commercial anti-virus software to scan its servers and desktops for unauthorized files and software. We selected a server to examine its virus-scan history for FY 2004. Virus scans were conducted for all other months of FY 2004, with the exception of April.

Investigation Of Potential Incidents Were Not Always Completed

FMS uses IDS logs and firewall logs to record its computer security incidents on its network. For the month of April 2004, we found that FMS identified two potential incidents investigated by CSIRC computer room staff. Although these two potential incidents were investigated, the two tickets were not completed as to the conclusion of the potential incident. Therefore, we were unable to determine the outcome of the investigations.

FMS's Software Patch Management Procedures Were Not Complete

FMS's IR established procedures for its software patch management process. We compared these procedures with the bureau software patch management requirements stated in TD P 85-01 and found that FMS's patch management procedures included all the requirements with the exception of the following areas:

- Server software shall be kept current with respect to security related system patches, modifications, and fixes.
- Only Treasury and/or bureau-approved software shall be used to access the Internet, and the software shall incorporate all vendor-provided security patches.

- Proper steps shall be taken to ensure that vulnerabilities discovered during penetration testing are repaired and that any damages possible in the interim are mitigated.

Appendix III to OMB Circular A-130, *Security of Federal Automated Information Resources*, requires that agencies establish, as part of a system security plan, an incident response capability. This capability should ensure that help is provided to users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats. This capability shall share information with other organizations, consistent with NIST coordination. Appendix III also requires that an agency should be able to respond in a manner that both protects its own information and helps to protect the information of others who might be affected by the incident. To address this concern, agencies should establish formal incident response mechanisms. Awareness and training for individuals with access to the system should include how to use the system's incident response capability.

The *Treasury Information Technology Security Program*, TD P 85-01, establishes comprehensive, uniform IT security policies to be followed by each bureau in developing its own specific policies and operating directives. The Treasury IT Security Program serves as a foundation for the bureaus' IT security programs. TD P 85-01 clarifies national policies, adapts them to Treasury's specific circumstances, and imposes additional requirements when necessary.

TD P 85-01 outlines procedures for an incident response capability designed to receive and disseminate incident information and provide a consistent capability to respond to and report on incidents. It also provides guidance to Treasury bureaus, Departmental Offices, the OIG, and the Treasury Inspector General for Tax Administration staff on responding to and reporting security incidents that affect Treasury's ability to conduct its mission. Specifically, TD P 85-01 provides for the following:

- A framework for identifying, handling, managing, responding to, and reporting incidents in a timely and expeditious fashion.

- A mechanism for disseminating generic and specific incident information to the CIOs and bureaus to ensure that actions are being taken to minimize the impact of ongoing or potential incidents.
- Government-wide information sharing of threats, incidents, and trends to support security planning and operations.

Without a complete CSIRC and software patch management function, FMS runs the risk of not accurately identifying and accounting for all its computer security incidents. As a result, FMS may understate mandated CSIRC reporting requirements, such as those identified as part of FISMA.

## Recommendations

The FMS CIO should ensure that:

1. Current FMS CSIRC policy and procedures are revised to incorporate bureau head responsibilities; and subsequent incidents are reported to TCSIRC.
2. All significant incidents identified by the Help Desk are reported to TCSIRC.
3. Help Desk tickets contain complete information; and follow-up tickets are generated for potential significant incidents identified by the Help Desk.
4. Virus scans are performed on a monthly basis.
5. All investigations of potential incidents identified by IDS and firewall logs are completed.
6. Software patch management procedures are revised to include the requirements regarding current server software related patches; approved software for accessing the Internet; and repairing and mitigating vulnerabilities discovered during penetration testing.

Management Response Management agreed with the recommendations and has implemented corrective measures to address them. These measures include (1) updating its Computer Security Incident Response Program Handbook, (2) ensuring Help Desk procedures incorporate appropriate incident reporting, (3) conducting regular virus scans, (4) revising Help Desk procedures

to ensure all tickets are closed, and (6) revising software patch management procedures.

OIG Comments The actions taken by FMS are responsive to the intent of our recommendations.

* * * * * *

I would like to extend my appreciation to the FMS staff for the cooperation and courtesies extended to my staff during the review. If you have any questions, please contact me at (202) 927-5774. Major contributors to this report are listed in Appendix 4.

/s/

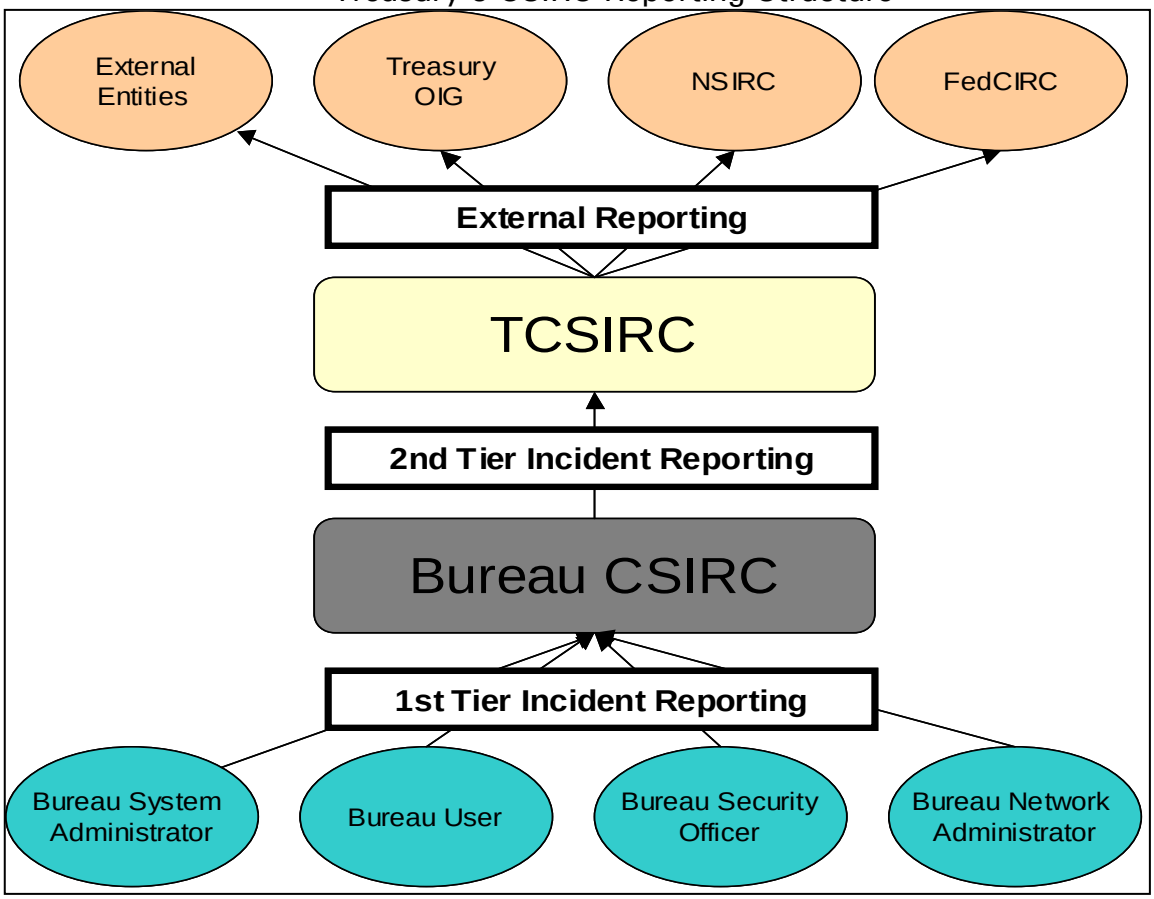
Louis C. King
Director, Information Technology Audits

The objective of this audit was to determine if FMS established an adequate CSIRC process. This objective was accomplished by determining if FMS established and implemented CSIRC policy and procedures compliant with Treasury and OMB criteria. We performed this audit by: (1) interviewing appropriate IT personnel; (2) obtaining and reviewing applicable CSIRC and software patch management process documentation; (3) obtaining and analyzing bureau level and Departmental level CSIRC data; and (4) observing bureau level and Departmental level CSIRC processes.

Our standards for CSIRC and software patch management performance for this audit were based solely on the bureau requirements published in Treasury Department Publication TD P 85-01 and OMB agency reporting requirements for FY 2003 FISMA.

This report details the fieldwork performed at the FMS site in Hyattsville, Maryland, from April through September 2004. We conducted our audit in accordance with generally accepted government auditing standards.

Treasury's CSIRC Reporting Structure[6]




*Source: Treasury IT Security Program (TD P 85-01)*

The TCSIRC serves as a 24 hours a day, 7 days a week, 365 days a year, escalation center and as the central point of contact for incidents within Treasury. The TCSIRC facilitates incident reporting to the Treasury OIG, and with external reporting entities. In addition, TCSIRC provides the following functions:

- A framework for identifying, handling, managing, responding to, and reporting computer incidents in a timely and expeditious manner.
- A mechanism for disseminating generic and specific computer security incident information to ensure that actions are being taken to minimize the impact of ongoing or potential incidents.
- Government-wide information sharing of threats, incidents, and trends to support computer security planning and operations.

[6] As of September 2003, the United States Computer Security Readiness Team (US-CERT) replaced FedCIRC in protecting the nation's Internet infrastructure against cyber attacks.

The following events are defined as computer security incidents and should be reported to TCSIRC:

| Computer Security Incidents | |
|---|---|
| Incident Type | Incident Description |
| Malicious Logic Attacks | Performed by crackers/hackers attempting to gain privileges and/or information, capture passwords, and modify audit logs to hide unauthorized activity. Attempts include viruses, Trojan horses, worms, and scripts. |
| Probes and Reconnaissance Scans | Includes probing or scanning networks for critical services or security weaknesses. |
| Unauthorized Access and Unsuccessful Attempts | All successful unauthorized accesses and suspicious unsuccessful attempts. |
| Denial-of-Service Attacks | Affect the availability of critical resources, such as e-mail servers, web servers, routers, gateways, and communication infrastructure. |
| Alterations/Compromises of Information | Involve the unauthorized altering of information or the compromise of information. |
| Adverse Site Mission Impacts | Significantly impact the mission of the site or operations. |
| Classified System Incidents | Involve either a system used to process national security information, or classified information on any system not certified for that level of classified information. |
| Loss or Theft of Equipment With Classified Information | Includes the compromise of user accounts and passwords allowing unauthorized persons access to Treasury computing resources, agents' names, or case information that could compromise an investigation or risk the loss of human life. Emphasis is on the data that was lost or stolen, not on the hardware itself. |
| Misuse of Resources | Misuse of a computing or telecommunications system or network by an authorized user. |
| Domain Name System Attacks | Affect the availability of services or networks. |
| Root Compromise | Compromise the most trusted privileges of the machines on the network. |
| Web Site Defacements | Superficial destruction of web pages that could cause embarrassment, but not lead to an attack. |
| | |

*Source: Treasury IT Security Program (TD P 85-01)*

DEPARTMENT OF THE TREASURY
FINANCIAL MANAGEMENT SERVICE
WASHINGTON, D.C. 20227

June 30, 2005

MEMORANDUM FOR LOUIS C. KING
DIRECTOR, INFORMATION TECHNOLOGY AUDITS

FROM: RICHARD L. GREGG

SUBJECT: Financial Management Service (FMS) Response to Draft Report on Review of FMS's Computer Security Incident Response Capability

Thank you for the opportunity to comment on the May 31, 2005 draft report entitled "FMS's Computer Security Incident Response Capability Needs Improvement." We have reviewed the draft audit report and are providing an update on corrective actions we have taken both during and since the audit was conducted. These include the following:

- FMS has updated its Computer Security Incident Response Program Handbook to incorporate your recommendations.
- FMS has ensured that its Help Desk procedures include reporting potential incidents to the FMS Computer Security Incident Response Program and to the Treasury Computer Security Incident Response Capability (TCSIRC) as required. In the case of the Help Desk tickets you cited as significant incidents, we have determined that these were not significant incidents, rather "false positives" and did not need to be reported to TCSIRC.
- FMS is conducting regular virus scanning. The problem identified was an operational anomaly and has not occurred since.
- Procedures have been revised to ensure that all Help Desk tickets are closed. This includes all potential incident investigations.
- FMS has revised our software patch management procedures in accordance with your recommendations.

We will continue to monitor our CSIRC, Help Desk, and Patch Management procedures to ensure they are being followed and will take further actions if needed.

cc: Donald Hammond

## Office of Inspector General

Louis C. King, Director
Joseph A. Maranto, III, IT Audit Manager
George Prytula, III, IT Audit Manager
Myung G. Han, Evaluator
Susan R. Sebert, Referencer

Department of the Treasury

Office of the Chief Information Officer
Office of Accounting and Internal Control

Financial Management Service

Office of the Chief Information Officer
Security Operations Directorate
Mission Assurance Directorate

Office of Management and Budget

Office of Inspector General Budget Examiner